

**UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH CAROLINA
CHARLESTON DIVISION**

FORTRA LLC and ECRIME
MANAGEMENT STRATEGIES INC. d/b/a
PHISHLABS,

Plaintiffs,

v.

DOPPEL INC. and PATRICK LELAND,

Defendants.

Case No.: 2:25-cv-03783-DCN

JURY TRIAL REQUESTED

COMPLAINT FOR INJUNCTIVE AND OTHER RELIEF

Plaintiffs Fortra LLC and Ecrime Management Strategies Inc., doing business as PhishLabs (collectively “PhishLabs” or “Plaintiffs”) bring this action for preliminary and permanent injunctive relief and monetary damages against former employee Patrick Leland (“Leland”) and his subsequent employer Doppel Inc. (“Doppel,” or together with Leland, “Defendants”). PhishLabs alleges as follows:

NATURE OF THE ACTION

1. This action asserts claims against Defendants for breach of contract, tortious interference with existing contracts and business relationships, and misappropriation of trade secrets, among other claims. These causes of action arise from the actions of Doppel—a direct competitor of PhishLabs—by unlawfully recruiting PhishLabs’ employees in South Carolina and elsewhere and misappropriating PhishLabs’ confidential information and trade secrets, including through Leland’s unlawful and unauthorized possession, misappropriation, and disclosure of PhishLabs’ confidential information and trade secrets in concert with and on behalf of Doppel.

2. Overall, Doppel's scheme centers on creating illicit shortcuts to more effectively (and efficiently) compete with its primary competitor, PhishLabs. Doppel has done so by, among other things, encouraging former PhishLabs employees to violate their agreements by indirectly soliciting PhishLabs employees to join Doppel. And Doppel has done so by having former PhishLabs employees make use of PhishLabs' highly confidential and trade secret documents and information on behalf of Doppel, including by sharing such information with other Doppel employees on the Slack messaging application at Doppel. This conduct—most of which took place *after* PhishLabs sent Doppel and several former employees of PhishLabs cease-and-desist letters in response to which Doppel assured PhishLabs it was doing nothing wrong—has allowed Doppel to fast-track its development of competing products and services by relying on the research and development done at PhishLabs rather than organically developing through its own trial and error and without the use of ill-gotten intellectual property of its competitors.

3. Indeed, in the days leading up to his leaving PhishLabs and joining Doppel in or around May 2024, Leland downloaded more than 400 PhishLabs files that he then took with him to Doppel. These files downloaded by Leland contain huge quantities of PhishLabs' confidential information and trade secrets, including the entire Shared Enterprises folder. The files Leland unlawfully stole included, among other things, the Roadmap (PhishLabs' primary, forward-looking business planning document) and several "Battle Cards" (PhishLabs' detailed internal analyses of how PhishLabs stacks up against its competitors in the marketplace).

4. Many of those files—which unequivocally contain PhishLabs' confidential information and trade secrets—were then posted internally at Doppel on various Slack channels for weeks and months at a time. Doppel also openly solicited former PhishLabs employees hired by Doppel to disclose confidential PhishLabs customer information to improve Doppel products

and services and to enable Doppel to solicit PhishLabs customers while using an unfair competitive advantage.

5. This shocking conduct gave Doppel's CEO Kevin Tian and other senior Doppel employees direct access to PhishLabs' most confidential information. For example, a Slack channel at Doppel included a posting of PhishLabs' internal "Roadmap," which is Doppel's primary, forward-looking business planning document detailing upcoming product and services research and innovation and customer initiatives. This Roadmap is part of the "secret sauce" for PhishLabs, as it contains detailed information regarding PhishLabs' forward-looking business (including how best to update its products and offerings together with specific details regarding client needs and requests). In other words, Doppel literally had PhishLabs' top-secret Roadmap posted internally for Doppel's team members to see, use, and copy. As another example, Doppel employees requested and discussed PhishLabs' pricing information via Slack. Plus, Tian knew about the posting of PhishLabs' confidential information and trade secrets at Doppel, and he either encouraged it or did little to stop it, as nobody at Doppel suffered sanctions for internally posting and relying on PhishLabs' confidential and trade secret information. In fact, the only Doppel employee who suffered any consequences with respect to this brazen misconduct appears to have been the individual who raised concerns regarding Doppel's possession of PhishLabs' confidential information and trade secrets.

6. All of this conduct—most of which was concealed from PhishLabs until a whistleblower came forward with information regarding Doppel's unlawful activity—enabled Doppel to jump years ahead of where it would have been absent its unlawful conduct. This conduct must stop. Unfortunately, however, Defendants continue to possess PhishLabs' confidential information and trade secrets, causing PhishLabs irreparable harm and significant damages.

Further, upon information and belief, Doppel intends to continue soliciting PhishLabs' employees (including by using a network of former PhishLabs employees who are now at Doppel) despite knowing that most of these employees are or were subject to non-solicitation and other restrictive covenant obligations to PhishLabs. To cease and prevent ongoing irreparable harm from Defendants' conduct, PhishLabs seeks preliminary and permanent injunctive relief, as well as monetary damages, attorneys' fees, and other available relief.

PROCEDURAL AND JURISDICTIONAL FACTS

The Parties

7. Plaintiff Fortra LLC is a Delaware limited liability company with its United States headquarters and principal place of business at 11095 Viking Suite Drive, Suite 100, Eden Prairie, Minnesota 45344.

8. Plaintiff Ecrime Management Strategies Inc. is a Delaware corporation and a subsidiary of Fortra LLC. Ecrime Management Strategies Inc. maintained its corporate headquarters at 1501 King Street, Charleston, South Carolina 29405 through December 31, 2024. Since January 1, 2025, Ecrime Management Strategies Inc. has maintained its corporate headquarters at 11095 Viking Suite Drive, Suite 100, Eden Prairie, Minnesota 45344. Ecrime Management Strategies Inc. continues to maintain significant business operations and employees in Charleston and throughout South Carolina.

9. Defendant Doppel is a Delaware corporation with its principal place of business at 440 North Barranca Avenue, Suite 5110, Covina, California 91723.

10. Defendant Leland is an individual citizen of South Carolina. Leland may be served at 4495 Cashiers Lane, North Charleston, South Carolina 29405 or wherever he may be found.

Jurisdiction and Venue

11. Pursuant to 28 U.S.C. § 1331, this Court has subject matter jurisdiction over this dispute because PhishLabs' claims under the Defend Trade Secrets Act ("DTSA"), 18 U.S.C. § 1836 *et seq.*, and the Lanham Act, 15 U.S.C. § 1051 *et seq.*, raise federal questions. PhishLabs' state law claims fall within the Court's supplemental jurisdiction pursuant to 28 U.S.C. § 1367, because the claims relate so closely to the federal questions that those claims form part of the same case or controversy.

12. PhishLabs consents to personal jurisdiction in this Court by filing this action.

13. The Court has personal jurisdiction over Leland because Leland resides in and is domiciled in the State of South Carolina. Further, Leland worked for PhishLabs in South Carolina, and he likewise worked for Doppel in South Carolina.

14. For the reasons more specifically described below, the Court has specific personal jurisdiction over Doppel for several reasons. First, Doppel employs multiple employees in South Carolina and has purposefully availed itself of the privilege of conducting activities in the forum, PhishLabs' claims arise out of those activities, and the exercise of personal jurisdiction is constitutionally reasonable. Second, Doppel is a "closely-related party" to Leland and therefore is subject to personal jurisdiction. Third, Doppel and Leland were active participants in a conspiracy, and substantially all of Leland's overt acts taken in furtherance of that conspiracy took place in South Carolina. Thus, Leland had sufficient contacts with the forum to subject Doppel to jurisdiction in this State.

15. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) and § 121 because a substantial part of the events or omissions giving rise to the claims at issue occurred in this District.

STATEMENT OF FACTS

PhishLabs is a Leading Innovator of Cybersecurity

16. Founded in 2008, PhishLabs is an innovative provider of cyber threat intelligence, digital risk protection, email incident response, and security awareness services and products. PhishLabs—a leader in the industry—develops and offers products and services including domain protection, brand protection, social media protection, data leak detection, account takeover protection, and advanced email protection. PhishLabs’ products protect enterprises, their brands, and their customers against digital risks including email-based threats such as spoofing and phishing. To develop cutting-edge products and services, PhishLabs performs deep investigation and analysis of the tactics, techniques and procedures used by threat actors to carry out attack campaigns. The Company also investigates the actors themselves and creates dossiers and reports for its customers and law enforcement agencies worldwide.

17. Top organizations worldwide trust PhishLabs to fight back against cyberattacks targeting their employees and their customers. Using a powerful combination of proprietary technology, specialized security operations, and deep threat intelligence, PhishLabs’ products and services are geared to detect threats early in the attack process and take rapid action to mitigate attacks before damage is done.

18. PhishLabs’ customers include top financial institutions, social media and career sites, healthcare companies, retail businesses, insurance companies, media and technology companies, and various other industries worldwide that are the target of serious cybercrime threats from individuals and state actors.

19. “Phishing” is the fraudulent practice of sending emails purporting to be from reputable sources to induce individuals or organizations to reveal personal information, such as

passwords and credit card numbers, or to gain illicit access to secured computer systems for purposes such as trade secret theft, corporate or political espionage, sabotage, or other nefarious reasons.

20. Many of PhishLabs' primary products and services are aimed at identifying, detecting, protecting against, and responding to phishing attacks.

21. In particular, PhishLabs specializes in researching and protecting against enterprise-focused phishing threats, and it is the leading provider of threat intelligence and mitigation solutions.

22. For example, PhishLabs provides a managed service known as its Phishing Incident Response service, which provides near real-time monitoring, expert analysis, and automated responses to user-reported emails.

23. In 2021, PhishLabs was acquired by HelpSystems LLC, later rebranded as Fortra, to expand its cybersecurity portfolio.

24. Fortra is an American cybersecurity company based in Eden Prairie, Minnesota. Founded in 1982 under the name Help/38, Fortra's mission is to help organizations increase security maturity while decreasing operational burden. Fortra offers a wide range of cybersecurity and automation products and services that provide its clients with data protection, infrastructure protection, digital risk and email security, security awareness training, and secure file transfer, among many other things. The PhishLabs Digital Risk Protection platform is one of Fortra's many industry-leading products.

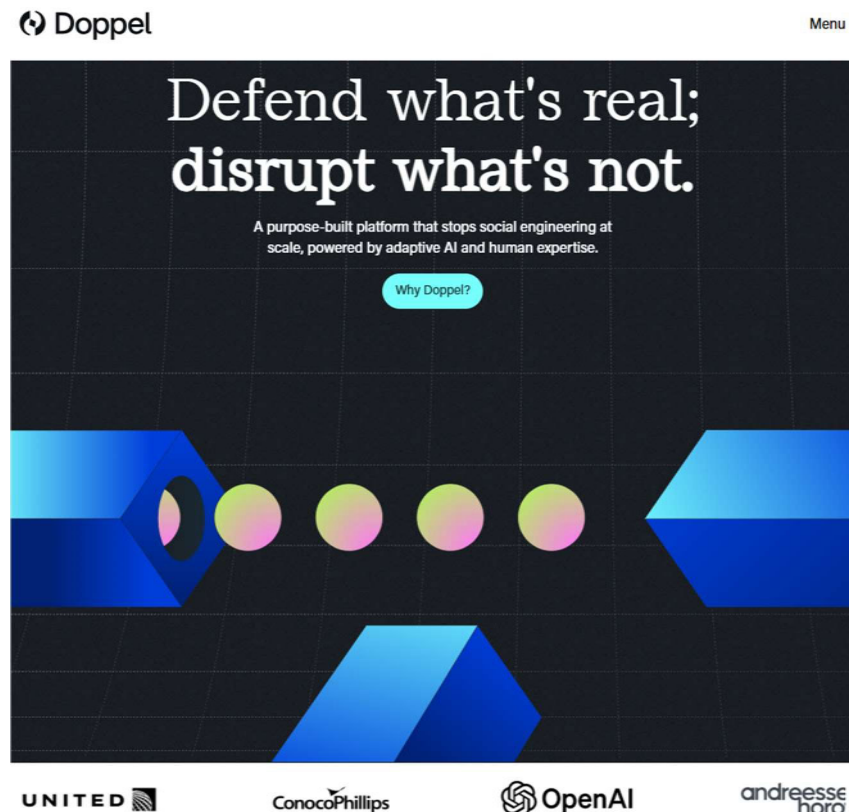
Doppel is a Direct Competitor of PhishLabs in a Highly-Competitive Industry

25. The cyber-intelligence and security industry serves a diverse group of customers. Due to the highly-specialized nature of the services provided by companies like PhishLabs together

with the tremendous amount of time and resources expended developing and improving cybersecurity products and services, there are few competitors in the market.

26. Founded in 2022—14 years *after* PhishLabs—Doppel is a direct competitor of PhishLabs. Doppel, like PhishLabs, is a cyber-intelligence and security company that serves clientele similar to the clientele served by PhishLabs. Like PhishLabs, Doppel offers products and services aimed at identifying, detecting, protecting against, and responding to phishing attacks to clients across the nation and around the globe.

27. Doppel's website¹ makes clear that it is a direct competitor of PhishLabs:



¹ See Doppel, <https://www.doppel.com/>.

Doppel Coverage

Solving disconnected defenses, protecting what matters.

Social engineering thrives on fragmentation. We connect the dots with the Doppel Vision Platform, unifying cross-channel intelligence into a single threat grid. By combining advanced LLM technology and expert human analysis, we eliminate blind spots, dismantle digital threats, and protect organizations at every level.

10k
Detected Threats

10M+
URLs Scanned


700k+
Social Accounts Scanned

100k+
Apps Scanned

Daily Average

Our Solutions

Disrupt social engineering at the source.



Brand Protection

Executive Protection

Safeguard leadership by preventing impersonation, phishing, and identity-based attacks on high-profile individuals.

[Learn More](#)

Email Resilience



28. Upon information and belief, Doppel is focused on growing its market share by, among other things, unlawfully recruiting PhishLabs' employees—including those who are subject to restrictive covenants—and using PhishLabs' confidential and trade secret information to unlawfully emulate PhishLabs' business model by interfering with PhishLabs' contracts and business relationships and by misappropriating its trade secrets and confidential information.

29. Although PhishLabs does not fear fair competition, Doppel—by and through its founders—is intentionally engaged in unfair competitive practices designed to accelerate its entry into the market and capture of market share from established competitors such as PhishLabs by poaching subject matter experts and client relationship managers from its main competitors. In doing so, Doppel seeks to systematically mine its competitors' former employees for confidential information, trade secrets, know-how developed by competitors, and other highly-sensitive

information relating to customers, products, services, and non-public information regarding cybersecurity threats and mitigation measures.

30. Upon information and belief, after hiring one or more of PhishLabs' former employees, Doppel elicited and obtained from those employees inside information regarding other PhishLabs' employees and obtained their collaboration in affirmatively contacting and soliciting additional PhishLabs' employees to join Doppel. Doppel did so while knowing those new employees at Doppel were still subject to restrictive covenant agreements with PhishLabs.

Leland's Employment with and Resignation from PhishLabs

31. In May 2022, PhishLabs hired Leland as an Associate Solutions Engineer in South Carolina.

32. As an Associates Solutions Engineer, Leland was responsible for, among other things:

- (a) understanding the specific cybersecurity challenges and requirements of PhishLabs' customers, including their current applications, access architecture, and desired security posture;
- (b) translating business requirements into technical solutions using PhishLabs' platforms and services, focusing on areas like domain monitoring, brand protection, and social media protection;
- (c) working closely with internal teams, including sales, product, engineering, and customer support, to ensure successful implementation and ongoing support solutions;
- (d) acting as a technical subject matter expert, providing guidance and recommendations to customers on best practices for cybersecurity and

PhishLabs solutions;

(e) demonstrating the value of PhishLabs solutions through presentations, demos, and proof-of-concept implementations; and

(f) staying current with the latest cybersecurity threats and trends, as well as new features and capabilities of PhishLabs' platforms.

33. PhishLabs placed a great deal of trust and confidence in Leland. In connection with his position as an Associates Solutions Engineer, Leland had access to secured databases and systems housing PhishLabs' trade secrets and confidential information. For example, Leland had access to the company's access-restricted "Shared Enterprises" network storage, which contained some of the company's most valuable confidential information and trade secrets.

34. On September 13, 2022, Leland signed a Confidentiality, Non-Competition and Assignment of Inventions Agreement with HS Topco, LP, an affiliate of Fortra and PhishLabs. (Ex. 1, Leland Confidentiality and Noncompetition Agreement.) The Leland Confidentiality and Noncompetition Agreement contains several restrictive covenants, three of which are relevant here.

35. First, the Leland Confidentiality and Noncompetition Agreement contains the following non-disclosure provision:

Obligation to Maintain Confidentiality. The Employee acknowledges that the information and data (including trade secrets) obtained by him or her during the course of his or her employment or other relationship ("Relationship") with the Company concerning the business or affairs of the Company ("Confidential Information") are the property of the Company, including information concerning acquisition opportunities in or reasonably related to the Company's business or industry of which the Employee becomes aware during his or her Relationship with the Company (the "Service Period"). Therefore, the Employee agrees that he or she will not disclose to any unauthorized individual, partnership, corporation, limited liability company, association of a joint stock company, trust, joint venture unincorporated organization, association or other entity, or a governmental entity (collectively, "Persons" or each individually a "Person") or use for his or her own

account or for the account or benefit of any other Person or entity any Confidential Information without the Company's written consent, unless and to the extent that the Confidential Information, (i) becomes generally known to and available for use by the public other than as a result of the Employee's acts or omissions to act or (ii) is required to be disclosed pursuant to any applicable law or court order. The Employee shall deliver to the Company upon termination of the Employee's Relationship with the Company for any reason whatsoever, regardless of the circumstances thereof, and including without limitation upon death, disability, retirement, discharge or resignation for any reason, whether voluntarily or involuntarily ("Termination Event"), or at any other time the Company may request, all tangible embodiments of Confidential Information, including all memoranda, notes, plans, records, reports, computer tapes, printouts and software and other documents and data (and copies thereof) relating to the Confidential Information, Work Product (as defined below) or the business of the Company to the extent containing Confidential Information which he or she may then possess or have under his or her control.

(*Id.* § 1(a).)

36. Second, the Leland Confidentiality and Noncompetition Agreement contains the following non-competition provision:

Noncompetition. During the Service Period and the one-year period immediately following the Service Period, (such period, together with the Service Period, is referred to herein as the "Restricted Period"), the Employee shall not, directly or indirectly, (A) own, manage, control, participate in, consult with, render services for, or in any manner engage in any business which competes anywhere in the United States or any other jurisdictions where the Company conduct business during the Service Period, with any of the businesses of the Company, or (B) engage in conduct that interferes or conflicts with the Employee's duties to the Company, or creates a potential business or fiduciary conflict.

(*Id.* § 2(a).)

37. Third, the Leland Confidentiality and Noncompetition Agreement contains the following non-solicitation provision:

Nonsolicitation. During the Restricted Period, the Employee shall not take any actions to, directly or indirectly through another entity, (i) induce or attempt to induce any employee of the Company to leave the employ of the Company, or in any way interfere with the relationship between the Company and any such employee thereof, (ii) hire any employee of the Company or hire any former employee of the Company within six (6) months after such person ceased to be an employee of the Company, (iii) induce or attempt to induce any customer, supplier,

licensee or other business relation of the Company to cease doing business with the Company or in any way interfere with the relationship between any such customer, supplier, licensee or business relation and the Company or (iv) acquire or attempt to acquire an interest in any business relating to the business of the Company and with which the Company has engaged in substantive discussions and negotiations relating to the acquisition of such business by the Company at any time within the one-year period immediately preceding a Termination Event; provided, however, that clause (i) will not apply to solicitation of any person if such solicitation was by way of general advertising or solicitation (such as a want ad in a newspaper of general circulation) not specifically directed to employees of the Company.

(*Id.* § 2(b).)

38. Leland further agreed to the enforcement of the restrictive covenants contained in the Leland Confidentiality and Noncompetition Agreement according to the following terms:

Enforcement. If, at the time of enforcement of Section 1 [Confidential Information] or this Section 2 [Noncompetition and Nonsolicitation], a court holds that the restrictions stated herein are unreasonable under circumstances then existing, the parties hereto agree that the maximum duration, scope or geographical area reasonable under such circumstances shall be substituted for the stated period, scope or area and that the court shall be allowed to revise the restrictions contained herein to cover the maximum duration, scope and area permitted by law. Because the Employee's services are unique and because the Employee has access to confidential information, the parties hereto agree that money damages would be an inadequate remedy for any breach of this Agreement. Therefore, in the event a breach or threatened breach of this Agreement, the Company and/or its respective successors or assigns shall be entitled to, in addition to other rights and remedies existing in their favor, specific performance and/or injunctive or other relief from a court of competent jurisdiction in order to enforce, or prevent any violations of, the provisions hereof (without posting a bond or other security). The Employee agrees that he/she shall not oppose the granting of an injunction, specific performance and/or other equitable relief to which the Company and/or its respective successors or assigns is expressly entitled on any basis, including the basis that any other party has an adequate remedy at law or that any award of an injunction, specific performance and/or other equitable relief is not an appropriate remedy for any reason at law or in equity.

(*Id.* § 2(c).)

39. Leland also acknowledged that the business of the company would take place throughout the United States and other jurisdictions (§ 2(d)) and that “the potential harm to the

Company of the non-enforcement of any provision of Section 1 or this Section 2 outweighs any potential harm to the Employee of its enforcement by injunction or otherwise” (§ 2(d)).

40. On or about April 6, 2023, Leland signed an Equity Tracking Unit Award Agreement Under the Halo Parent Newco, LLC 2021 Equity Tracking Unit Plan (“Leland Equity Agreement”), under which Leland was granted a sum-certain of Equity Tracking Units. (Ex. 2, Leland Equity Agreement.) Plaintiff Fotra LLC is a subsidiary of Halo Parent Newco, LLC.

41. In exchange for the grant of Equity Tracking Units under the Leland Equity Agreement, Leland agreed to the following additional non-solicitation provision:

Nonsolicitation. The Grantee acknowledges that in the course of his or her Service Relationship with the Company, 2019 HS TopCo, LP, or any of their Subsidiaries (including, without limitation, prior to the date hereof) he or she has, and will continue to, become familiar with the Company’s, 2019 HS TopCo, LP’s and their respective Subsidiaries’ trade secrets and with other confidential information concerning the Company, 2019 HS TopCo, LP, and such Subsidiaries and that his or her services will be of special, unique and extraordinary value to the Company, 2019 HS TopCo, LP, and such Subsidiaries. Therefore, the Grantee agrees that:

a. Nonsolicitation. During his or her Service Relationship with the Company, 2019 HS TopCo, LP, or any of their respective Subsidiaries (the “Service Period”) and the one year period immediately following the Service Period, (such period, together with the Service Period, is referred to herein as the “Restricted Period”), the Grantee shall not take any actions to, directly or indirectly through another entity anywhere in the United States or any other jurisdictions where the Company, 2019 HS TopCo, LP, or any of their respective Subsidiaries conduct business, (i) induce or attempt to induce any employee of the Company, 2019 HS TopCo, LP, or any of their respective Subsidiaries to leave the employ of the Company, the Company or such Subsidiary, or in any way interfere with the relationship between the Company, 2019 HS TopCo, LP, or any of their respective Subsidiaries and any such employee thereof, (ii) hire any employee of the Company, 2019 HS TopCo, LP, or any of their respective Subsidiaries or hire any former employee of the Company, 2019 HS TopCo, LP, or any of their respective Subsidiaries within six (6) months after such person ceased to be an employee of the Company, 2019 HS TopCo, LP, or any of their respective Subsidiaries, (iii) induce or attempt to induce any customer, supplier, licensee or other business relation of the Company, 2019 HS TopCo, LP, or any of their respective Subsidiaries to cease doing business with the Company, 2019 HS TopCo, LP, or such Subsidiary or in any way interfere with the relationship between any such

customer, supplier, licensee or business relation and the Company, 2019 HS TopCo, LP, or any such Subsidiary or (iv) acquire or attempt to acquire an interest in any business relating to the business of the Company, the Company or any of their respective Subsidiaries and with which the Company, 2019 HS TopCo, LP, or any of their respective Subsidiaries has engaged in substantive discussions and negotiations relating to the acquisition of such business by the Company, 2019 HS TopCo, LP, or any of their respective Subsidiaries at any time within the one-year period immediately preceding the termination of the Grantee's Service Relationship with the Company, 2019 HS TopCo, LP, and their respective Subsidiaries for any reason whatsoever, regardless of the circumstances thereof, and including without limitation upon death, disability, retirement, discharge or resignation for any reason, whether voluntarily or involuntarily; provided, however, that clause (i) will not apply to solicitation of any person if such solicitation was by way of general advertising or solicitation (such as a want ad in a newspaper of general circulation) not specifically directed to employees of the Company, 2019 HS TopCo, LP, or any of their respective Subsidiaries.

(*Id.* § 5.)

42. Leland agreed to an enforcement provision under the Leland Equity Agreement which is substantially similar to that under the Leland Confidentiality and Noncompetition Agreement. (*Id.* § 5(b).) And he further acknowledged and agreed that the business of the company would take place throughout the United States and other jurisdictions. (*Id.* § 5(c).)

43. The Leland Equity Agreement contains an integration clause which expressly provides that “any prior agreement entered into between Grantee and Company, 2019 HS TopCo, LP, or any of their respective Subsidiaries, containing obligations relating to confidentiality, non-solicitation, non-competition or similar agreements shall remain in full force and effect in accordance with its terms.” (*Id.* § 9.)

Leland's Separation from PhishLabs and Subsequent Employment with Doppel

44. Upon information and belief, prior to May 30, 2024, Leland was contacted and recruited by Doppel and/or its agents for the purpose of soliciting Leland to come to work for Doppel in a competitive capacity with PhishLabs.

45. On May 30, 2024, Leland voluntarily resigned from PhishLabs.

46. Immediately prior to resigning from PhishLabs on May 30, 2024 to join Doppel, Leland downloaded nearly 400 files—approximately 1 terabyte in data—containing PhishLabs’ confidential information and trade secrets. Leland did so after entering into employment discussions with Doppel and in the days leading up to his resignation from PhishLabs. Leland was not authorized to download any of these files for his own purposes. Moreover, Leland had no legitimate business reason to access the vast majority, if not any, of these files when he accessed them; thus, Leland exceeded the scope of what he was authorized to access by accessing and downloading those files. PhishLabs did not learn about this massive downloading of 1 terabyte in data until almost a year later in April 2025.

47. Leland officially started his employment with Doppel as a Sales Engineer in May 2024. However, upon information and belief, Leland was clandestinely acting as Doppel’s agent and for his own unlawful purposes prior to the official commencement of his employment with Doppel. Thus, Leland was gathering PhishLabs’ confidential information and trade secrets both for his own benefit as well as to benefit his new employer, Doppel. And Leland did so to gain an unlawful competitive advantage over PhishLabs with respect to its competitive products and services, as well as with respect to its existing and prospective customers.

48. Upon information and belief, Leland’s job duties for Doppel were the same or similar to the job duties he performed for PhishLabs.

Leland’s Access to PhishLabs Confidential Information and Trade Secrets

49. Given the cutting-edge technology on which PhishLabs relies in conducting its business, preventing unfair and unlawful competition and misappropriation of confidential information and trade secrets is paramount to PhishLabs’ business. As such, PhishLabs invests

substantial time, money, and other resources to develop its confidential information and trade secrets.

50. As an Associate Solutions Engineer at PhishLabs (and prior to joining Doppel), Leland had access to a great deal of highly-confidential information and trade secrets—information which PhishLabs vigorously protects from competitors. For example, PhishLabs permitted Leland to access, and he regularly used, the following categories of PhishLabs’ confidential information and trade secrets in performing his job duties:

- (a) customer lists and related information, including customer contact information, pricing and budgetary information, and customer needs and/or requirements, among other things;
- (b) vendor lists, including pricing information and related information;
- (c) information relating to contracts between PhishLabs and its customers;
- (d) PhishLabs’ pricing models;
- (e) competitive intelligence regarding PhishLabs’ competitors;
- (f) account strategies regarding PhishLabs’ past and/or current customers;
- (g) PhishLabs’ highly confidential “Roadmap” document;
- (h) PhishLabs’ highly confidential “Battle Cards”;
- (i) PhishLabs’ monthly summary dashboard template as designed for customers, which took significant resources to create and which included a visual overview of security activity for a specific client, the severity level of the activity, how many incidents were active, how many incidents were closed; and
- (j) PhishLabs’ organization and marketing and growth strategies.

51. The above-referenced confidential information and trade secrets, all of which

PhishLabs authorized Leland to access while serving as an employee of PhishLabs for the limited purpose of conducting PhishLabs' business, are highly sensitive, commercially valuable, and would be useful to Doppel and other competitors in their efforts to compete with PhishLabs.

52. PhishLabs takes extensive precautions to protect its confidential information and trade secrets provided to associates like Defendant. For example, PhishLabs has established extensive computerized password and information security protocols and requires associates to sign agreements (such as Leland's restrictive covenant agreements) in which they agree not to disclose such information and to refrain from engaging in unfair competition in which they might be able to use such information. PhishLabs maintains policies and procedures with respect to the confidentiality of its records and intellectual property. Moreover, PhishLabs secures its network from unauthorized access with additional security features, such as multi-factor authentication.

53. Accordingly, the above-referenced trade secrets and confidential information are not generally known to the public.

54. With access to such highly sensitive confidential information and trade secrets, Leland—and Doppel—have the knowledge necessary to engineer a strategy to unlawfully compete with PhishLabs.

Doppel's Unlawful Recruitment of Plaintiffs' Current and Former Employees

55. Beginning in 2024, Doppel began a systematic campaign to poach PhishLabs' employees. Doppel hired *at least* eight current or former employees of PhishLabs—all of whom were subject to restrictive covenant agreements—between April and July 2024:

- (a) Davis Craig, a former Threat Detection Specialist who went to work for Doppel as a Solutions Architecture Manager beginning in July 2024;
- (b) Bryce Delbridge, a former Senior Security Analyst who went to work for Doppel

as a Security Analyst II/Provider Relations and Escalation Specialist beginning in June 2024;

(c) Esther Hiott, a former Associate Manager, Security Operations, who went to work for Doppel as a Security Operations Center (SOC) Manager beginning in 2024;

(d) Jadon Hiott, a former Security Operations Lead, who went to work for Doppel as a Security Operations Center (SOC) Manager beginning in April 2024;

(e) Defendant Patrick Leland, who started with Doppel as a Sales Engineer in May 2024;

(f) Jesse Levy, a former Account Representative who went to work for Doppel as an Account Executive beginning in April 2024;

(g) Evan Luck, a former Account Executive who went to work for Doppel as an Account Executive beginning in May 2024;

(h) Scott Roman, a former Associate Manager, Security Operations, who went to work for Doppel as a Senior Manager, Security Operations beginning in May 2024; and

(i) Tim Sawyer, a former Senior Customer Success Manager who went to work for Doppel as an Enterprise Client Success Manager beginning in May 2024.

56. Upon information and belief, each of the above-referenced former employees of PhishLabs performed the same or substantially similar job duties at Doppel as those job duties that each of them performed at PhishLabs. Further, each of the above-referenced former employees had access to PhishLabs' confidential information and trade secrets.

57. Notably, Craig Davis, Esther Hiott, Jadon Hiott, Leland, Evan Luck, Scott Roman, and Tim Sawyer resided in South Carolina when they worked for PhishLabs, when they applied for and/or were recruited by Doppel, and during their terms of employment with Doppel.

58. With respect to Sawyer, in the spring of 2024, Tian reached out to Sawyer to solicit him to work for Doppel in South Carolina. Doppel's CTO Rahul Madduluri and Customer Success Manager Lisa Chong had a series of phone calls with Sawyer after the initial solicitation by Tian. Doppel offered Sawyer a position in South Carolina by email following these calls. After Sawyer was hired, Doppel employees sent property (such as company laptops) to Sawyer in South Carolina, engaged in Zoom meetings and phone calls with its South Carolina-based employees, and paid any taxes in South Carolina related to its South Carolina-based employees in accordance with South Carolina law.

59. Upon information and belief, Doppel actively encouraged Scott Roman and Esther Hiott to actively recruit PhishLabs employees in South Carolina and elsewhere to resign from PhishLabs and go to work for Doppel, with Doppel ultimately offering hiring multiple PhishLabs employees to work for Doppel in South Carolina and other states. Because Roman and Hiott have restrictive covenant agreements with PhishLabs that are substantially similar to the Leland Confidentiality and Noncompetition Agreement and the Leland Equity Agreement (including prohibitions against directly or indirectly soliciting employees), Doppel was thus encouraging Roman and Hiott to directly violate the restrictive covenant agreements between PhishLabs (on the one hand) and Roman and Hiott (on the other). (Ex. 3 Roman Confidentiality and Noncompetition Agreement; Ex. 4, Roman Equity Agreement; Ex. 5, Hiott Confidentiality and Noncompetition Agreement; Ex. 6, Hiott Equity Agreement.)

60. Plaintiffs further assert that one or more of PhishLabs' former employees made unlawful attempts—at Doppel's direction—to solicit PhishLabs' customers, in direct violation of their respective restrictive covenant agreements.

61. Upon information and belief, former PhishLabs employees hired by Doppel have

solicited and are continuing to solicit PhishLabs' customers for the benefit of Doppel, despite Doppel's awareness of the restrictive covenants contained in each of their respective restrictive covenant agreements.

62. Taken together, it is clear that Doppel—a company founded nearly a decade and a half after PhishLabs—sought to recruit current and former employees of PhishLabs in order to give it a head start by leveraging the trade secrets and intellectual property of its competitor. This is unfair and unlawful. PhishLabs asserts, upon information and belief, that the unlawful recruitment of PhishLabs' current and former employees allowed Doppel to jump years ahead of where it would have been absent its unlawful conduct.

63. In furtherance of its unlawful scheme, Doppel posted false information regarding PhishLabs and its capabilities on its website. Indeed, Doppel posted the following putative comparison between PhishLabs and Doppel:

Switching to Doppel?		
	Doppel	PhishLabs
Unlimited Takedowns For domains, brands, and execs	✓	✓
Advanced Domains Detection of subdomain, content-based cases	✓	✓
AI-Native Detection LLMs for detection, takedowns, and intel	✓	✗
Challenging Takedown Resolution Ex-Silicon Valley team with strategic relationships	✓	✗
Emerging Channels Coverage Crypto, global platforms, messaging apps, dark markets	✓	✗
Fast Domain Takedowns Enabled by Google Safe Browsing and Cloudflare Partnerships	✓	✗
24/7 Real-Time Support Via e-mail, Slack, Teams, Telegram, Discord, and more	✓	✗

64. The above information is false and misleading. For example, Doppel claimed that PhishLabs does not have emerging channels coverage (including crypto, global platforms, messaging apps, and dark markets). This is false and was known by Doppel to be false, including through the former PhishLabs employees Doppel recruited and employed. PhishLabs' services cover all of these channels.

65. Doppel also claimed that PhishLabs does not have fast domain takedowns enabled by Google Safe Browsing and Cloudflare partnerships. Again, this is completely false and was known to be false by Doppel. PhishLabs does have fast domain takedowns, utilizes Google Safe Browsing, and has a direct business relationship with Cloudflare. Moreover, PhishLabs also has 24/7 real-time support, challenging takedown resolution, and hundreds of strategic relationships.

66. On June 10, 2024—as soon as practicable after learning about some (but not all) of the above-mentioned misconduct—PhishLabs' legal counsel sent letters to Leland, Roman, and Hiott, among other former PhishLabs employees, reminding them of their respective obligations under the terms of their restrictive covenant agreements with PhishLabs. (Ex. 7, Reminder Letter to Leland; Ex. 8, Reminder Letter to Roman; Ex. 9, Reminder Letter to Hiott.)

67. On June 20, 2024, PhishLabs sent a cease-and-desist letter to Doppel, addressed to its Chief Executive Officer, Kevin Tian. (Ex. 10, Cease and Desist to Doppel.) This letter advised Doppel that it had hired multiple former PhishLabs employees, all of whom were subject to restrictive covenant agreements, and noted that PhishLabs was aware that Roman and Hiott were blatantly violating their restrictive covenant agreements by actively recruiting PhishLabs' employees. Crucially, the letter stated as follows:

To the extent Doppel was unaware of these contractual obligations to Fortra, **it is hereby on notice that these employees—and many others—have post-employment obligations to Fortra and are expected to abide by them.** Any involvement by Doppel in breaches of former Fortra/PhishLabs employees'

agreements will therefore subject it to liability for tortious interference with contract.

(*Id.* (emphasis in original).)

68. PhishLabs' June 20, 2024 letter also demanded that Doppel remove the unlawful misrepresentations regarding its products from Doppel's website. (*Id.*)

69. On July 16, 2024, counsel for Doppel sent a letter responding to PhishLabs' earlier cease-and-desist letter, which states, in relevant part, as follows:

[I]n the interest of bringing this matter to a close, we hereby represent that the former Fortra/PhishLabs employees referenced in your letter have been instructed, not to: (1) solicit Fortra/PhishLabs employees; (2) solicit Fortra/PhishLabs customers; and (3) disclose or use Fortra/PhishLabs confidential information or trade secrets in connection with their employment with Doppel. Doppel fully expects that the employees will comply with these instructions. Doppel has removed the content regarding PhishLabs on its website referenced in your letter.

(Ex. 11, July 16, 2024 Response Letter from Doppel.)

Doppel Allows and Actively Encourages Further Unlawful Conduct

70. In the wake of receiving PhishLabs' June 20, 2024 cease-and-desist letter, Doppel's CEO Tian called a meeting with all of the former PhishLabs employees who had received letters regarding their obligations under restrictive covenant agreements.

71. In this meeting, Tian did not tell these employees to stop soliciting PhishLabs' employees. Instead, Tian merely suggested that these former PhishLabs employees run solicitation efforts through him so that he could target and reach out to those PhishLabs employees.

72. Otherwise stated, Tian encouraged Doppel employees, including those employed by Doppel in South Carolina, to indirectly solicit PhishLabs employees in violation of their Agreements with PhishLabs in order to better shield their unlawful activities from detection by PhishLabs in light of PhishLabs' cease-and-desist demands.

73. In doing so, Tian and Doppel doubled down on their tortious conduct and efforts to compete directly with PhishLabs by taking shortcuts and accelerating Doppel's development via hiring PhishLabs' talented employees to obtain confidential and trade secret information.

74. Despite PhishLabs' earlier warnings to Doppel and Hiott, Hiott continued engaging in efforts on Doppel's behalf to unlawfully solicit PhishLabs' employees and business relationships and/or using PhishLabs' confidential information. On August 1, 2024, PhishLabs sent Hiott a cease-and-desist letter demanding that Hiott not engage in any further conduct in violation of her restrictive covenant agreements. (Ex. 12, Aug. 1, 2024 Cease and Desist to Hiott.)

75. In the months that followed, many of the former PhishLabs employees who went to work for Doppel would regularly—and openly—discuss PhishLabs' confidential and proprietary information on Doppel's internal Slack channels, including information regarding PhishLabs' pricing information, methodologies, and agreements between PhishLabs and its third-party vendors. For example, Sammir Samman—Doppel's head of sales—directly asked Roman whether he had “data on Phishlabs PIR pricing” on at least one occasion. By way of another example, Bryce Delbridge shared information with Doppel employees and representatives regarding special business relationships and arrangements PhishLabs had developed with key strategic partners in its business, and Delbridge suggested that Doppel do the same.

76. But the misappropriation and dissemination of PhishLabs' confidential information and trade secrets on Doppel's internal Slack channels went far beyond mere discussion. Although PhishLabs did not learn about Doppel's conduct until March 2025, Leland regularly shared highly confidential PhishLabs documents (that he unlawfully stole from PhishLabs) on Doppel's corporate systems, including its internal Slack channels, including:

(a) PhishLabs' internal Roadmap document, which contains detailed information

regarding PhishLabs' forward-looking business plans, including specific requests made by certain of Phishlabs' customers was posted on Slack at Doppel; and

- (b) The DRP Samples web app monthly_summary document ("PhishLabs Monthly Summary"), which is a proprietary dashboard template designed by PhishLabs for customers and which provided a monthly visual overview of key security activity, was posted on Slack at Doppel.

77. In the summer of 2024, Sawyer, a former PhishLabs employee, saw that Leland was disseminating PhishLabs' confidential information and trade secrets. As a result, he immediately contacted Tian and advised Tian that Doppel should not be using or sharing such information belonging to PhishLabs. Tian stated that the information would be taken down. But that did not happen in its entirety. Indeed, Sawyer noticed that some of the confidential information and trade secrets at issue were still available on Doppel's internal Slack channels as late as January 2025.

78. On January 31, 2025, Doppel terminated Sawyer's employment—after Sawyer raised issues regarding the misappropriation of PhishLabs' confidential information and trade secrets. Upon information and belief, Sawyer received South Carolina unemployment insurance benefits from Doppel following his employment termination.

79. In March 2025, Sawyer contacted PhishLabs and informed PhishLabs of some of the aforementioned unlawful conduct he observed while working for Doppel and that Doppel had failed to remove confidential PhishLabs information from its internal Slack channels after Sawyer made an internal whistleblower complaint about the same to Doppel's CEO.

80. After learning about the theft and misappropriation of its confidential information and trade secrets, PhishLabs began an internal investigation and forensic review of its own systems in late March 2025 and continuing into April 2025.

81. Through its investigation, PhishLabs discovered that on May 14, 2024, Leland had downloaded at least approximately 400 files containing approximately 1 terabyte of data, some or all of which he saved to a personal USB storage device with the serial number 0C70011410B0. The files Leland downloaded contain huge quantities of PhishLabs' confidential information and trade secrets, including the entire Shared Enterprises folder. The files Leland unlawfully stole included, among other things, the Roadmap, the PhishLabs Monthly Summary, and several iterations of PhishLabs' internal "Battle Cards," which are detailed internal analyses of PhishLabs' competition and competitive advantages in the marketplace not shared with anyone outside select individuals in the organization.

82. Thus, it was not until March and April 2025, that PhishLabs knew or could have known about Doppel's unlawful acquisition and use of its trade secrets and confidential information.

83. Upon information and belief, PhishLabs' confidential information and trade secrets are still located on Doppel's internal computer systems, including on Doppel's Slack channels.

84. Further, Doppel is targeting PhishLabs' customers and performing various trials for those customers, and (upon information and belief) those trials are using confidential information obtained from former PhishLabs employees at Doppel, including information from the PhishLabs Roadmap, PhishLabs pricing information, details regarding customer engagements with PhishLabs, and other confidential PhishLabs documents and information shared internally with Doppel personnel, including on Doppel's Slack channels.

85. Upon information and belief, Leland is violating and will continue to violate, the restrictive covenants contained in the Leland Equity Agreement and the Leland Confidentiality and Noncompetition Agreement by, among other things, using or disclosing PhishLabs' confidential information and trade secrets, soliciting PhishLabs' employees, and/or soliciting PhishLabs' clients and prospective clients.

86. Upon information and belief, Leland and Doppel are using, and will continue to use, PhishLabs' confidential information and trade secrets to unfairly—and unlawfully—compete with PhishLabs.

87. PhishLabs has been and, unless Doppel and its agents are stopped, will continue to be harmed as a direct result of the Defendants' unlawful conduct.

88. Plaintiffs have suffered damages as a result of Defendants' wrongful acts detailed herein, including but not limited to the loss of customer business and injury to PhishLabs' goodwill. For example, but without limitation, Plaintiffs have suffered lost revenue in excess of \$200,000 per year from just one of its customer relationships as the result of Defendants actions.

89. Upon information and belief, Doppel intends to continue to emulate PhishLabs' business model by, among other things, poaching current and former employees of PhishLabs to gain access to PhishLabs' confidential information and trade secrets to unlawfully compete with it.

CAUSES OF ACTION

Count I – Breach of Contract **(Leland)**

90. PhishLabs hereby repeats, re-alleges, and incorporates by reference the allegations contained in paragraphs 1-89 above as if fully set forth herein.

91. The restrictive covenants contained in the Leland Confidentiality and Noncompetition Agreement and the Leland Equity Agreement are valid and enforceable contractual obligations between Leland and PhishLabs. PhishLabs bargained for, and gave valuable consideration for, the restrictive covenants contained in those contracts.

92. Leland's employment with Doppel violated the noncompetition provision in the Leland Confidentiality and Noncompetition Agreement because Leland accepted a position with Doppel—a competitor of PhishLabs—during the prohibited time period.

93. Moreover, by downloading and disseminating PhishLabs' confidential information and trade secrets, Leland unequivocally breached the non-disclosure provision in the Leland Confidentiality and Noncompetition Agreement.

94. Finally, PhishLabs alleges, upon information and belief, that Leland has solicited PhishLabs' employees and customers in violation of the non-solicitation provisions in both the Leland Confidentiality and Noncompetition Agreement and the Leland Equity Agreement.

95. By breaching these valid and enforceable contractual provisions, Leland has caused irreparable harm to PhishLabs' business reputation and its relationships with its existing and potential customers and existing employees, harm from unfair competition, and harm from the unlawful disclosure and use of PhishLabs' confidential information and trade secrets.

96. Upon proving these breaches and the consequent damages, PhishLabs will seek all damages and other relief recoverable for Leland's breaches.

Count II – Violations of the DTSA
(All Defendants)

97. PhishLabs hereby repeats, re-alleges, and incorporates by reference the allegations contained in paragraphs 1-89 above as if fully set forth herein.

98. While employed by PhishLabs, Leland had access to PhishLabs' confidential and proprietary information—which constitute trade secrets under the DTSA—including client information, pricing and business strategy information, the Roadmap, sales strategies and techniques, marketing strategies and information, and other financial information (including many of the approximately 400 PhishLabs documents downloaded by Leland), among other things discussed above.

99. PhishLabs derives independent economic value from its confidential and proprietary information not being known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.

100. PhishLabs' trade secrets are used in, or intended for use in, interstate commerce.

101. PhishLabs expended substantial time, effort, money, and resources in acquiring, developing and maintaining its confidential and proprietary information.

102. PhishLabs takes reasonable, affirmative measures to maintain the confidentiality of this information for PhishLabs' exclusive benefit and competitive advantage in the industry.

103. Leland had, and has, a duty not to use or disclose PhishLabs' trade secrets for his own benefit or for that of a competitor.

104. Leland and Doppel have wrongfully acquired, retained, and/or disclosed PhishLabs' trade secrets through improper means.

105. Defendants have been unjustly enriched as a proximate result of the misappropriation of PhishLabs' trade secrets.

106. Defendants' actions were and continue to be willful and malicious.

107. As a direct and proximate result of Defendants' misappropriation of PhishLabs' trade secrets, PhishLabs has suffered, and will continue to suffer, irreparable harm and economic damages. PhishLabs is thus entitled to actual damages and disgorgement of any amount by which Defendants have been unjustly enriched, in amounts to be proven at trial, together with punitive damages, together with injunctive relief, compensatory damages, exemplary damages, and attorneys' fees.

Count III – Violations of the South Carolina Trade Secrets Act
(All Defendants)

108. PhishLabs hereby repeats, re-alleges, and incorporates by reference the allegations contained in paragraphs 1-89 above as if fully set forth herein.

109. While employed by PhishLabs, Leland had access to PhishLabs' confidential and proprietary information—which constitute trade secrets under the South Carolina Trade Secrets Act, S.C. Code § 39-8-10 *et seq.*—including client information, pricing and business strategy information, the Roadmap, sales strategies and techniques, marketing strategies and information, and other financial information (including many of the approximately 400 PhishLabs documents downloaded by Leland), among other things discussed above.

110. PhishLabs derives independent economic value from its confidential and proprietary information not being known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.

111. PhishLabs expended substantial time, effort, money, and resources in acquiring, developing and maintaining its confidential and proprietary information.

112. PhishLabs takes reasonable, affirmative measures to maintain the confidentiality of this information for PhishLabs' exclusive benefit and competitive advantage in the industry.

113. Leland had, and has, a duty not to use or disclose PhishLabs' trade secrets for his own benefit or for that of a competitor.

114. Leland and Doppel have wrongfully acquired, retained, and/or disclosed PhishLabs' trade secrets through improper means.

115. Defendants have been unjustly enriched as a proximate result of the misappropriation of PhishLabs' trade secrets.

116. Defendants' actions were and continue to be willful and malicious.

117. As a direct and proximate result of Defendants' misappropriation, PhishLabs has suffered, and will continue to suffer, irreparable harm and economic damages. PhishLabs is thus entitled to actual damages and disgorgement of any amount by which Defendants have been unjustly enriched, in amounts to be proven at trial.

118. Defendants acted willfully, wantonly, and/or in reckless disregard of Plaintiffs' rights in their violations of the South Carolina Trade Secrets Act, and consequently Plaintiffs are further entitled to separate exemplary damages in an amount of twice any award for actual damages in accordance with S.C. Code § 39-8-40(C). PhishLabs is further entitled to an injunction against actual or threatened misappropriation under S.C. Code § 39-8-50.

119. Based on Defendants' willful misappropriation, Plaintiffs are entitled to an award of its reasonable attorneys' fees in accordance with S.C. Code § 39-8-80.

Count IV – Tortious Interference with Contract
(Doppel)

120. PhishLabs hereby repeats, re-alleges, and incorporates by reference the allegations contained in paragraphs 1-89 above as if fully set forth herein.

121. The restrictive covenant agreements between PhishLabs (on the one hand) and the former employees identified in paragraph 55 (on the other) constitute valid and enforceable

contracts which generally prohibit those individuals from working for a competitor of PhishLabs for a certain period of time, soliciting PhishLabs' customers or employees for a certain period of time, or using or disclosing PhishLabs confidential information and trade secrets.

122. Doppel was aware no later than June 20, 2024, of the restrictive covenant agreements between the former employees identified in paragraph 55, on the one hand, and PhishLabs, on the other. Despite this knowledge, Doppel continued actively encouraging indirect and, upon information and belief, direct violations of the restrictive covenants contained in those agreements. Indeed, Tian encouraged indirect solicitation by having former PhishLabs employees who had employee non-solicit obligations to PhishLabs route new candidates to him.

123. PhishLabs has been directly and proximately injured as the direct result of Doppel's interference. PhishLabs is entitled to monetary damages, in an amount to be proven at trial, and preliminary and permanent injunctive relief arising from Doppel's unlawful conduct.

Count V – Breach of Contractual and Common Law Duties of Loyalty
(Leland)

124. PhishLabs hereby repeats, re-alleges, and incorporates by reference the allegations contained in paragraphs 1-89 above as if fully set forth herein.

125. As an employee of PhishLabs, Leland owed PhishLabs a duty to remain faithful to its interests throughout his employment both under the terms of the applicable contract and under the common law.

126. "It is implicit in any contract for employment that the employee shall remain faithful to the employer's interest throughout the term of employment." *Berry v. Goodyear Tire & Rubber Co.*, 270 S.C. 489, 491, 242 S.E.2d 551, 552 (1978).

127. Leland also owed PhishLabs a duty not to engage in disloyal acts in aid of future competition with PhishLabs.

128. By engaging in the conduct described above, Leland took actions directed at competing with PhishLabs prior to his resignation.

129. PhishLabs has been directly and proximately injured as the direct result of Leland's actions. PhishLabs is entitled to monetary damages, in an amount to be proven at trial, and all other remedies available under applicable law.

Count VI – Violations of the Lanham Act
(Doppel)

130. PhishLabs hereby repeats, re-alleges, and incorporates by reference the allegations contained in paragraphs 1-89 above as if fully set forth herein.

131. Doppel posted a series of misleading and blatantly false statements about PhishLabs on its website. The statements were material and were likely to influence the purchasing decisions of customers and potential customers.

132. Doing so constitutes false advertising in violation of the Lanham Act. Specifically, the Lanham Act prohibits, among other things, individuals and entities from using false representations in the advertisement of the sale of good or services. *See* 15 U.S.C. § 1125(a).

133. Notably, “both false advertising of a competitor’s products and false advertising of one’s own products are actionable.” *C.B. Fleet Co. v. SmithKline Beecham Consumer Healthcare, L.P.*, 131 F.3d 430, 434 (4th Cir. 1997).

134. Doppel’s false and misleading statements were made intentionally and willfully.

135. PhishLabs is entitled to recover all damages available under 15 U.S.C. § 1117 as a result of Doppel’s misrepresentations, including Doppel’s profits, any actual damages sustained, and the costs of the action.

Count VII – Unfair Trade Practices
(All Defendants)

136. PhishLabs hereby repeats, re-alleges, and incorporates by reference the allegations contained in paragraphs 1-89 above as if fully set forth herein.

137. Pursuant to S.C. Code § 39-5-20 *et seq.*, Defendants' conduct, as set forth throughout the Complaint, constitutes an unfair method of competition and unfair and deceptive trade acts or practices in the conduct of trade or commerce which had an adverse impact on the public interest being that the conduct has the potential for repetition.

138. Defendants' purpose in taking these damaging and costly actions was to afford Doppel an unfair competitive advantage over PhishLabs, including permitting Doppel to benefit at the expense of PhishLabs from the improper misappropriation, use and inevitable use of PhishLabs' trade secrets, interfering with PhishLabs' relationships and contractual agreements with its employees, and gaining an unfair advantage in obtaining a head start in its operations from not having to experience the same trial and errors that PhishLabs experienced in the many years since its founding.

139. Upon information and belief, Doppel is using or intends to use PhishLabs' confidential information and trade secrets and the key employees it has solicited away from PhishLabs in order to assist Doppel in designing and manufacturing products and services that will directly compete with the products offered by PhishLabs.

140. Doppel knew or should have known of Leland's wrongful acts.

141. Defendants' conduct and actions have adversely affected the industry for the products at issue and its customers and have and will continue to impact on the public interest.

142. Defendants' conduct constitutes a willing and knowing violation of S.C. Code § 39-5-20 *et. seq* and has and will continue to proximately cause damage to PhishLabs.

143. Pursuant to S.C. Code § 39-5-140, PhishLabs is entitled to recover from Defendants such damages as it may prove at trial and to have those damages trebled. In addition, PhishLabs is entitled to recover its reasonable attorneys' fees and costs pursuant to S.C. Code § 39-5-140.

Count VIII – Civil Conspiracy
(All Defendants)

144. PhishLabs hereby repeats, re-alleges, and incorporates by reference the allegations contained in paragraphs 1-89 above as if fully set forth herein.

145. Upon information and belief, the Defendants knowingly and willfully agreed and conspired between themselves to perform the acts pled in the Complaint, and each Defendant adopted, approved, and ratified the wrongful acts of the other.

146. Over a period of time, upon information and belief, Defendants have engaged in a deliberate course of conduct for the unlawful purpose of causing serious irreparable injury to PhishLabs' business by misappropriating, using and inevitably using trade secrets and confidential information of PhishLabs about its business, customers, products, processes, equipment designs and business relationships and soliciting away PhishLabs' key employees, and have developed competing products and services with knowledge of such information to the competitive disadvantage of PhishLabs.

147. Upon information and belief, PhishLabs engaged in a common plan to injure PhishLabs' business and to secure business for the benefit of Doppel.

148. Upon information and belief, Defendants communicated, planned and colluded by telephone and/or other means, to bring about their plan to injure PhishLabs' business.

149. By their collective actions, substantially all of which occurred in or were otherwise directed at South Carolina, Defendants have caused greater harm to PhishLabs than either could

have individually caused, resulting in separate injury to PhishLabs which would not have occurred but for their concerted actions.

150. The recurring improper conduct of Defendants has been the actual and proximate cause of PhishLabs' injuries.

151. These wrongful acts by Defendants have caused PhishLabs actual and punitive damages separate from and above the other actual damages alleged herein and have caused and continue to cause irreparable harm to PhishLabs for which such legal damages are insufficient.

Count IX – Unjust Enrichment
(All Defendants)

152. PhishLabs hereby repeats, re-alleges, and incorporates by reference the allegations contained in paragraph 1-89 above as if fully set forth herein.

153. Defendants' improper conduct alleged above, including their misappropriation of and use and/or threatened or inevitable use of PhishLabs' confidential information and trade secrets has enabled and will continue to enable Doppel to compete unfairly with PhishLabs, including permitting Doppel to gain a head start in its operations from not having to experience the same trial and errors that PhishLabs experienced by PhishLabs.

154. These actions were wrongful and performed in a malicious manner to harm PhishLabs and to unjustly enrich Defendants at PhishLabs' expense.

155. As a direct and proximate result of Defendants' improper conduct alleged above, Doppel has been unjustly enriched in an amount to be determined at trial, and PhishLabs is entitled to the disgorgement of any and all profits, earnings and commissions attributable to Defendants' wrongful actions.

REQUEST FOR RELIEF

PhishLabs respectfully requests that this Court enter judgment for Plaintiffs and against Defendants as follows:

A. Temporarily, preliminarily and permanently enjoining Defendants from acquiring, accessing, using, disclosing, or misappropriating PhishLabs' confidential information and trade secrets and award against Defendants all of PhishLabs' compensatory damages, exemplary damages, punitive damages, costs and attorneys' fees resulting from such misappropriation;

B. Temporarily, preliminarily and permanently enjoining Leland from continuing to violate any of his obligations under his restrictive covenant agreements, whether on behalf of himself, Doppel, or some other employer or entity;

C. Temporarily, preliminary and permanently enjoining all Defendants from interfering with PhishLabs' customers, business, and contracts, including contracts between PhishLabs and its employees and customers;

D. Ordering Defendants to immediately return to PhishLabs any and all of PhishLabs' electronic and hardcopy confidential information and/or trade secrets and to take all steps necessary to effectuate a forensic examination of any and all devices capable of performing computing functions or storing electronic information that are owned by, have been used by, or been accessible to Leland at any time since the date six months prior to the date on his employment with PhishLabs terminated through the present for the purpose of determining how he accessed, used, disclosed, or misappropriated PhishLabs' confidential information and/or trade secrets;

E. Granting PhishLabs access to any and all personal accounts used for communication purposes by Leland so that PhishLabs may determine the extent to which he (1)

retained, used, or disclosed any of PhishLabs' confidential information and/or trade secrets, and/or (2) took other actions toward violating his obligations the restrictive covenant agreements;

F. Granting PhishLabs access to any and all devices owned, used or accessed by Leland for the purpose of determining if such devices contain copies of PhishLabs' confidential information and/or trade secrets, and permitting PhishLabs to take any other appropriate and reasonable steps to recover its confidential information and/or trade secrets and to ensure none of PhishLabs' confidential information or trade secrets were distributed or preserved by any of the Defendants, in any form;

G. Restraining the Defendants from in any way divulging, disseminating, or utilizing PhishLabs' confidential information and/or trade secrets in the interim;

H. Awarding against both Defendants actual damages, lost profits, and disgorgement, in an amount to be proven at trial, together with exemplary damages, punitive damages, costs and attorneys' fees, pre- and post-judgment interest, plus any other damages available under applicable law and permanent injunctive relief; and

I. Providing such further relief as the Court deems just under the circumstances.

Dated: May 5, 2025.

Respectfully submitted,

**OGLETREE, DEAKINS, NASH, SMOAK
& STEWART, P.C.**

/s/ Michael Oliver Eckard

Michael Oliver Eckard (Fed. I.D. #12055)

211 King Street, Suite 200

Charleston, SC 29401

Telephone: (843) 853-1300

Facsimile: (843) 853-9992

Michael.eckard@ogletree.com

ATTORNEY FOR PLAINTIFFS